ACEEE Int. J. on Recent Trends in Engineering and Technology, Vol. 10, No. 2, Jan 2014

Security Enhancement in AODV Routing Protocol for MANETs

Basavaraj S. Sannakashappanavar[1], C R. Byrareddy[2], Ravikumar M. Inamathi[2]
[1] Annasaheb Dange College of Engineering & Technology, Ashta, India
Email: raj.ec008@gmail.com
[2] Bangalore Institute of Technology, Bangalore, India
Email: byrareddycr@yahoo.co.in
[3] M.S.Bidve Engineering College, Lattur, India
Email: raviinamathi038@gmail.com

***Abstract*— Adhoc networks are a new wireless networking paradigm for mobile hosts. Mobile Ad-hoc Networks (MANETs) are wireless networks with absence of infrastructure centralized support. Routing in MANETs is challenging task due to mobility of nodes. Several routing protocols have been developed for Mobile Ad-hoc Networks. This paper describes concept of security enhancement in AODV routing protocol by detection and tolerance of attacks using secure message transmission (SMT) protocol. Present AODV routing protocol is not secure by malicious nodes. One main challenge in design of these networks is their vulnerability to security attacks. In this paper we study how to make node malicious and at same we will detect malicious node in AODV protocol using Network Simulator-2(NS-2) tool.**

***Index Terms*— AODV, AdHoc, NS-2(Network Simulator 2)**

I. INTRODUCTION

Mobile ad hoc networks (MANETs) have become a prevalent research area over the last couple of years. Many research teams develop new ideas for protocols, services, and security applicable for these type of networks. This is mainly due to the specific challenges and requirements MANETs pose on the protocols and mechanisms used. They require new concepts and approaches to solve the networking challenges. MANETs consist of mobile nodes which can act as sender, receiver, and forwarder for messages. They communicate using a wireless communication link e.g. a Wireless LAN (WLAN) adapter (IEEE 802.11). These networks are subject to frequent link breaks which also lead to a constantly changing network topology. Due to the specific characteristics of the wireless channel, the network capacity is relatively small. Hence, to be able to use MANETs with many nodes, very effective and resource efficient protocols are needed.

Mobile Ad-hoc networks are self-organizing and self-configuring multi-hop wireless networks. The structure of the network changes dynamically due to mobility of nodes, interference and path loss. Nodes in these networks utilize the same random access wireless links, cooperating in an intimate manner to engaging themselves in multi-hop forwarding. The node in the network not only acts as hosts but also as routers that route data to and from other nodes in network. Since the nodes are independent to move in any direction, there may be frequent link breakage. In MANET all network activities like discovering the topology and delivering messages must be executed by the nodes themselves. Hence routing functionality

DOI: 01.IJRTET.10.2.510

will have to be In corporate into the mobile nodes. The performance of nodes in ad-hoc networks is critical, since the amount of available power for excessive calculation and radio transmission are constrained. Such a network may operate in a standalone fashion, or may be connected to the larger Internet. Mobile nodes can directly communicate to those nodes that are in radio range of each other, whereas others nodes need the help of intermediate nodes to route their packets.

Routing in MANETs is challenging task due to mobility of nodes. Routing is the process of finding desire destination and transferring information to required destination. There may be many attacks like denial of attack, black hole attack etc during transmission of data. so security is main task to detect these attacks. Several routing protocols have been developed for Mobile Ad-hoc Networks. This paper describes concept of enhancement in detection and tolerance of attacks using secure message transmission (SMT) protocol. Here we propose the secure message transmission (SMT) protocol to safeguard the data transmission against arbitrary malicious behaviour of network nodes. SMT is a lightweight, yet very effective, protocol that can operate solely in an end-to-end manner. It exploits the redundancy of multi-path routing and adapts its operation to remain efficient and effective even in highly adverse environments. Here we compare and evaluate performance of normal AODV and with SMT protocol AODV.

MANETs dealing with many challenges while designing protocols. There are routing, security and reliability, Quality of service, inter-networking, power consumption.

Routing: Routing is one of the major issue, Since the topology of the network is constantly changing, the issue of routing packets between any pair of nodes becomes a challenging task. Most protocols should be based on reactive routing instead of proactive. Multi cast routing is another challenge because the multi cast tree is no longer static due to the random movement of nodes within the network. Routes between nodes may potentially contain multiple hops, which is more complex than the single hop communication.

Security and Reliability: In addition to the common vulnerabilities of wireless connection, an ad hoc network has its particular security problems due to e.g. nasty neighbour relaying packets. The feature of distributed operation requires different schemes of authentication and key management. Further, wireless link characteristics introduce also reliability problems, because of the limited wireless transmission range, the broadcast nature of the wireless medium, mobility-induced packet losses, and data transmission errors.

Quality of Service (QoS): Providing different quality of service levels in a constantly changing environment will be a challenge. The inherent stochastic feature of communications quality in a MANET makes it difficult to offer fixed guarantees on the services offered to a device.

Inter-networking: In addition to the communication within an ad hoc network, inter-networking between MANET and fixed networks (mainly IP based) is often expected in many cases. The coexistence of routing protocols in such a mobile device is a challenge for the harmonious mobility management.

Power Consumption: For most of the light-weight mobile terminals, the communication-related functions should be optimized for lean power consumption.

In this paper we study comparison of normal MAODV and SMT protocols in terms of performance metrics such as overhead, Total overhead, packet delivery ratio by varying number of connections. The simulation is carried out using Network Simulator-2.26, Awk scripts are used to calculate values of performance metrics.

In order to establish routes between nodes which are farther than a single hop, specially configured routing protocols are engaged. The unique feature of these protocols is their ability to trace routes in spite of a dynamic topology.

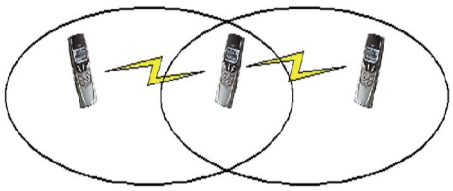

Figure 1. Infrastructure less networks

Fig.1 illustrates a simple 3-node ad-hoc network. In this figure, a source node wants to communicate with a destination node. Source and Destination are not within transmission range of each other. Therefore, they both use the relay node R to forward packets from one to another. So, even though R is primarily a host, R is acting as a *router* at the same time.

II. LITERATURE SURVEY

The following list of papers discuses routing in ad-hoc network:
The paper [1] explain Secure routing protocols for mobile ad hoc networks which are vital to proper wireless network operation. Unfortunately, ad hoc protocol security properties are often unknown and difficult to analyze. The paper [2] surveys research in service advertising, discovery and selection for mobile ad hoc networks and related issues. It includes a categorization of service discovery architectures for MANETs and their modes of operation, presenting their merits and drawbacks.
The paper [3] gives review of protocols with a particular focus on security aspects. The protocols differ in terms of routing methodologies and the information used to make routing decisions. The paper [4] deals energy conservation and scalability are probably two most critical issues in designing protocols for multi hop wireless networks, because wireless devices are usually powered by batteries only and have limited computing capability while the number of such devices could be large.
The paper [5] explains Mobile Ad-Hoc Networks (MANETs) are particularly useful and well-suited for critical scenarios, including military, law enforcement as well as emergency rescue and disaster recovery. The paper [6] deals with for broadcast operation in wireless ad hoc network to prevent collision and achieve low latency at the same time. Here it discuses a greedy broadcast scheduling algorithm based on the graph theory of Maximum Weight Independent Set (MWIS) problem.
The paper [7] it analyzes the robustness of the original AODV and AODV-BR and pointed out their shortcomings. In this paper, we analyze the Ad-hoc On-demand Distance Vector (AODV) routing protocol. Then it explains a Robust AODV protocol, where the route is built on demand and maintained by locally updating route information. The paper [8] deals with two routing protocols named DSDV and AODV are simulated and compared under specific scenarios with WSNs environment.
The paper [9] explains mobile ad hoc networks, there is no centralized infrastructure to monitor or allocate the resources used by the mobile nodes. The absence of any central coordinator makes the routing a complex one compared to cellular networks. The paper [10] presents the modifications of the AODV protocol for dynamic ad-hoc networks. With this modification, they can achieve loner lifetime with stable route without any central information about topologies or traffic demands.
The paper [11] explains study of attacks that are possible in Ad-Hoc networks faces and means to model the same in Network Simulator-2.

III. PROPOSED WORK

In chapter 1, an introduction to secured routing in ad-hoc networks is discussed. An exhaustive literature survey in different allied domains is also included. This chapter presents methodology for proposed work.

A. Network Architecture

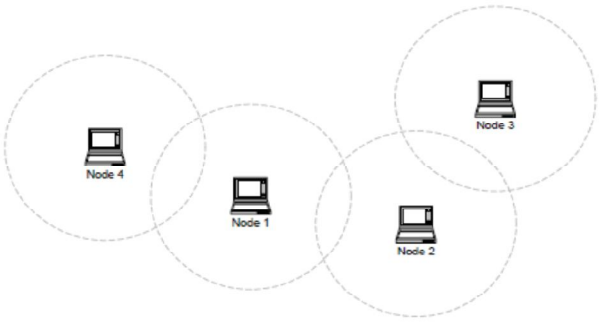

Figure 2. Mobile Ad-Hoc Networks

As above Fig .2 gives Mobile ad-hoc network architecture with random motion of mobile nodes, in which each node will have range. If any node contact between two rang node will activate to transfer the data. Here as shown above Node1, Node2, Node3 and Node4 are mobile nodes which have range between other nodes.
It includes sender that transmits the information required destination. Initially network is ideal until unless we request to particular source to find destination for data transmission.

Mobile Ad hoc networks are infrastructure less networks with dynamically changing topology. Several on demand routing protocols have been proposed to facilitate the communication in these network. In our project we enabled Multicast routing in AODV protocol. The multicast operation of the Ad hoc On-Demand Distance Vector (MAODV) routing protocol is intended for use by mobile node in an ad hoc network. It offers quick adaptation to dynamic link conditions, low processing and memory overhead, and low network utilization. It creates bi-directional shared multicast trees connecting multicast sources and receivers. These multicast trees are maintained as long as group members exist within the connected portion of the network. Each multicast group has a group leader whose responsibility is maintaining the group sequence number, which is used to ensure freshness of routing information

When we initiate the request, source will activate and it will check preferable disjoint node, at same time RREQ message is sent to all nodes with verified signature. All receiver receives the RREQ message and set reverse path to source. If any unknown behaviour found SMT Agent will detect the attackers and tolerate from attackers. RREP message sent back to the source after getting shortest path. Here node will move randomly within the given range. This is how network scenario will operates with secure data transmission.

B. MAODV Routing Protocol

The multicast operation of the Ad hoc On-Demand Distance Vector (MAODV) routing protocol is intended for use by mobile node in an ad hoc network. It offers quick adaptation to dynamic link conditions, low processing and memory overhead, and low network utilization. It creates bi-directional shared multicast trees connecting multicast sources and receivers. These multicast trees are maintained as long as group members exist within the connected portion of the network. Each multicast group has a group leader whose responsibility is maintaining the group sequence number, which is used to ensure freshness of routing information

The multicast Ad hoc On Demand Distance Vector (MAODV) is a reactive, on demand protocol. It builds routes between nodes only as desired by source nodes. It maintains these routes as long as they are needed by the sources. It uses sequence numbers to ensure the freshness of routes. It is loop-free, self-starting and scales to large numbers of mobile nodes.

MAODV builds routes using a route request / route reply query cycle. When a source node desires a route to a destination for which it does not already have a route, a route request (RREQ) packet is flooded across the network as shown in Fig.3. Nodes receiving this packet update their information for the source node and set up backwards pointers to the source node in the route tables. In addition to the source node's IP address, current sequence number, and broadcast ID, the RREQ also contains the most recent sequence number for the destination of which the source node is aware. In case of Multicast support Ad-hoc On Demand Distance Vector node transmitting a RREQ message sends that message on all interfaces which have been configured for operation in the ad-hoc network instead of broadcasting that message across the network.

Following are the message format used in MAODV.

MAODV Message Formats:

MAODV is reactive protocol, when a node wishes to start transmission with another node in the network to which it has no route; MAODV will provide topology information for the node. MAODV use control messages to find a route to the destination node in the network.

Following are the types of control messages in MAODV which are discussed bellow.

Route Request Message (RREQ):

Source node that needs to communicate with another node in the network transmits RREQ message. AODV floods RREQ message, using expanding ring technique. There is a time to live (TTL) value in every RREQ message, the value of TTL states the number of hops the RREQ should be transmitted.

The parameters contained in the route request packet are presented in the Fig.3 below for AODV:

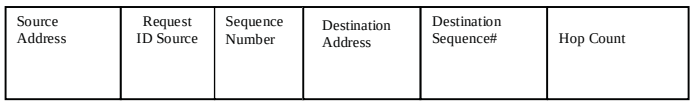

Figure 3. Route Request

Multicast RREQ contains addition fields as follows:

Join flag (J): Set when source node wants to join a multicast group.

Repair flag(R): set when a node wants to initiate a repair to connect two previously disconnected portions of the multicast tree. When a node wishes to repair a multicast tree, it appends the Multicast Group Rebuild extension. When a node wishes to unicast the RREQ for a multicast group to the group leader, it includes the Multicast Group Leader extension.
*Route Reply Message (RREP):*A node having a requested identity or any intermediate node that has a route to the requested node generates a route reply RREP message back to the originator node.
The parameters contained in the route reply message are presented in the Fig.4 for AODV

Source address	Destination address	Destination Sequence#	Hop count

Figure 4. Route Reply

Multicast RREP contains addition fields as follows:
Group Leader IP: The group leader broadcasts periodical a Group Hello message (RREP, the group sequence number is incremented for every Group Hello message)
Hop Count to next group member: The group sequence number is incremented for every Group Hello message to each member.
Repair flag: set when a node is responding to a repair request to connect two previously disconnected portions of the multicast tree. When the RREP is sent for a multicast destination, the Multicast Group Information extension is appended.
*Route Error Message (RERR):*Every node in the network keeps monitoring the link status to its neighbour's nodes during active routes. When the node detects a link crack in an active route, (RERR) message is generated by the node in order to notify other nodes that the link is down.
Multicast Activation Message (MACT):
Join flag (J): set when a node is joining the multicast group, as opposed to finding a route to the group for the transmission of data messages.
Prune flag (P): set when a node wishes to prune itself from the tree, unset when the node is activating a tree link.
Group Leader flag (G): set by a multicast tree member that fails to repair a multicast tree link breakage, and indicates to the group member receiving the message that it should become the new multicast group leader.
Update flag (U): set when a multicast tree member has repaired a broken tree link and is now a new distance from the group leader.
Reboot flag(R): set when a node has just rebooted.
Hop Count: The distance of the sending node from the multicast group leader. Used only when the 'U' flag is set, otherwise sent as 0.
Multicast Group IP Address: The IP address of the Multicast Group for which a route is supplied.
Source IP Address: The IP address of the sending node.
Source Sequence Number: The current sequence number for route information generated by the source of the route request.
To prune itself from the tree (i.e., inactivate its last link to the multicast tree), a multicast tree member sends a MACT with the 'P' flag = 1 to its next hop on the multicast tree. A multicast tree member that has more than one next hop to the multicast tree should not prune itself from the multicast tree.
Group Hello Message (GRPH):
Update flag (U): set when there has been a change in group leader information.
Off_Mtree flag (O): set by a node receiving the group hello that is not on the multicast tree.
Group Leader IP Address: The IP address of the group leader.
Hop Count: The number of hops the packet has travelled. Used by multicast tree nodes to update their distance from the group leader when the M flag is not set.
Multicast Group IP Address: The IP address of the Multicast Group for which sequence number is supplied.
Multicast Group Sequence Number: The current sequence number of the multicast group.
Route Maintenance:
A route established between source and destination pair is maintained as long as needed by the source. If the source node moves during an active session, it can reinitiate route discovery to establish a new route to destination. However, if the destination or some intermediate node moves, the node upstream of the break

remove the routing entry and send route error (RERR) message to the affected active upstream neighbours. These nodes in turn propagate the RERR to their precursor nodes, and so on until the source node is reached. The affected source node may then choose to either stop sending data or reinitiate route discovery for that destination by sending out a new RREQ message. In case of multiple interface AODV when a node needs to transmit a RERR, it should only transmit it on those interfaces which have precursor nodes for that route.

Routing Table:

The following information is stored in each entry of the multicast route table for multicast tree routes:

Multicast Group IP Address: IP Address of the particular group to which we sending information.

Multicast Group Leader IP Address: IP Address of the particular group leader which will maintain groups in the network.

Multicast Group Sequence Number: Sequence number of particular group.

Hop Count to Multicast Group Leader: Each group leader maintains hop count of each other member in that group for data transmission.

Join flag: To join a Multicast Group send a RREQ with the join flag set to the address of the group.

Destination IP: IP Address of the Destination node.

Destination sequence number: Sequence number for this Destination.

Next hop: The neighbour, which has been designed to forward packets to the destination for this route entry.

Hop Count: Number of hops to the destination.

Active neighbours List: Neighbour nodes that are actively using this route entry.

Expiration time/Lifetime: The time for which route is considered valid.

C. Description of Project Work

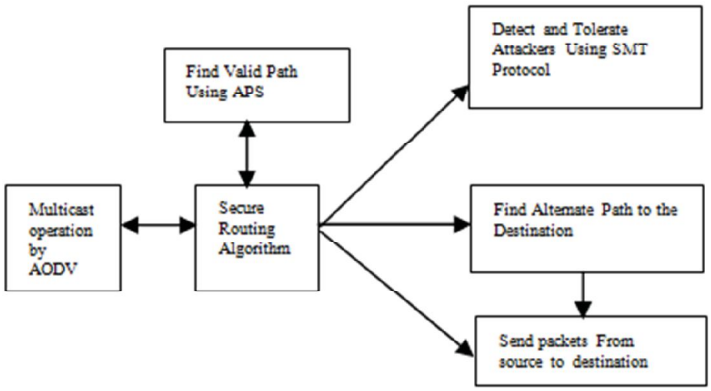

Figure 5. Proposed Models

Proposed solution here for attackers is to detect and tolerate them using SMT protocol by finding more than one route to the destination. The receiver and the malicious in addition to any intermediate node might have a route to the destination will reply to this ping request. The source will check those acknowledgements, and process them in order to figure out which one is not safe and might have the malicious node. Every packet in MANETs has a unique sequence number. This number is an increasing value, i.e., the next packet must have higher value that the current packet sequence number.

Initially after route discovery by multicast operation at any particular time, the two communicating end nodes make use of a set of diverse, preferably node disjoint paths that are deemed valid at that time. We refer to such a set of paths as the active path set (APS). If any malicious nodes present SMT Agent will detect immediately and find optimized path using SMT protocol. By this secure transmission of information made for communication.

In Fig.5 shows our proposed models in which AODV is get operated with multicast operation, using secure routing algorithm it finds valid path which is called active path set (APS).The algorithm detects and tolerates attackers by using SMT protocol, if any attacks found then algorithm finds Different path to transmit packets from source to destination.

D. Proposed Algorithm

Algorithm MAODV with SMT protocol

Step 1: Start at source, Multicast RREQ to nodes, to pass message through their neighbors to nodes with which they cannot directly communicate.
Step 2: MAODV does this by discovering the routes along which messages can be passed by Multicast operation.
Step 3: Initialize Active Path Set →(APS) operation, the two communicating end nodes make use of a set of diverse, preferably node disjoint paths that are deemed valid at that time.
Step 4: Source start updating APS Rating.
Step 5: At intermediate nodes, verify destination sequence no.
If destination Sequence Number (Node) < destination Sequence Number (packet):
Update routing table entry with this path and broadcast this packet
Else send RREP to source.
Step 6: SMT protocol gets operated if any unknown behaviour.
Step7: Any attacks detected, SMT agent sends ACK to tolerate from attacks.
Step8: Successful messages are received from destination, If not then route is broken or compromised.
Step9: If node gets more than one RREQ from same source then:
If (node! = destination)
Discard RREQ
If (node=destination)
Process RREQ
Step10: Stop APS Operation.
Step11: Reconstruct Message as Original using Security Association (SA) by MAC.
Step12: Compare all RREQ at destination on some attribute value like latency or number of hops and selects RREQs to process and discard rest.
Step13: Create RREP for all collected RREQ and process them towards source.
Step 14: At intermediate nodes, for multiple entries by RREP from same destination, preserve the entries coming from different nodes, delete rest duplicate entries.
Step15: At source node after getting multiple RREP Forward data using single path. Forward data using multiple paths.
Step16: If RERR is received by source for some path, Delete the entry of concerned path from routing table. Consider the other path as primary or as needed.
Step17: Stop SMT Protocol.
Step 18: Step 1 continue for next Communication.
Above algorithm explains working of MAODV with SMT protocol for secure data transmission over the network. It consists of step by step procedure from starting route discovery to end of transmission of data to desire destination.
In multicast environment there are many groups. Each group contains nodes, nodes called member of that group. Among which contain group leader for each group and group leader maintain members within that group. So RREQ is sent to all group leaders, leader will find destination within that group.
Initially whenever request is given to source to find destination it will initiate the RREQ, which contains destination address, source address and destination sequence number of packet to be sent to find destination. This process is called route discovery. In multicast RREQ sent to all group within that network, such that it will sent to all other members within that group.
With SMT, at any particular time, the two communicating end nodes make use of a set of
diverse, preferably node disjoint paths that are deemed valid at that time. We refer to such a set of paths as the active path set (APS). The source first invokes the underlying route discovery protocol, updates its network topology view, and then determines the initial APS for communication with the specific destination. Sequence number of each packet is compare with sequence number present in routing table to avoid loops within network.
SMT protocol gets operated if any unknown behaviour and make secure data transmission.
It will detect any attacks found while transferring the data and tolerate from dropping of packets. This is how routine will continue for all communication and make secure data transmission.

E. Case Study

In the Fig.6 above shows a set up of four nodes on a wireless network. The circles illustrate the range of communication for each node. Because of the limited range, each node can only communicate with the nodes

next to it. Here node 1 wants to send message to node 3, whenever it comes to the range sends information to destination.

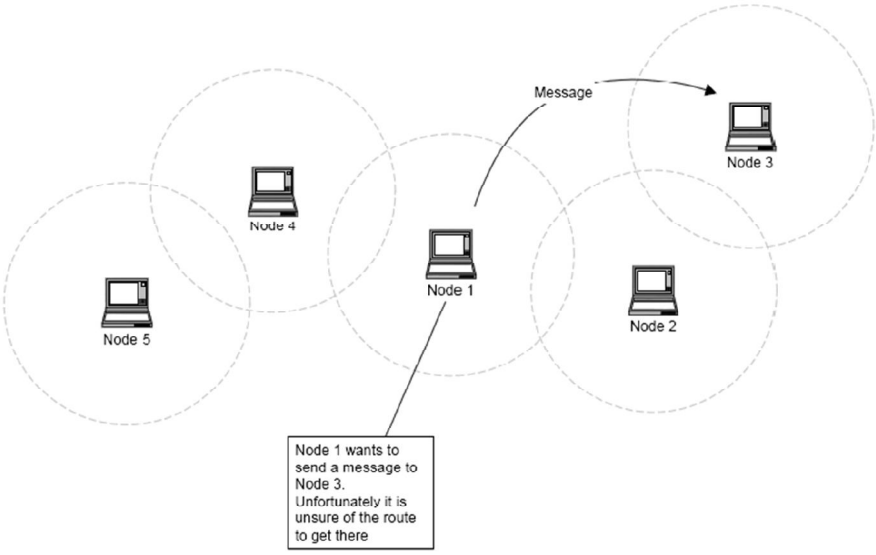

Figure 6. Nodes in Wireless Network

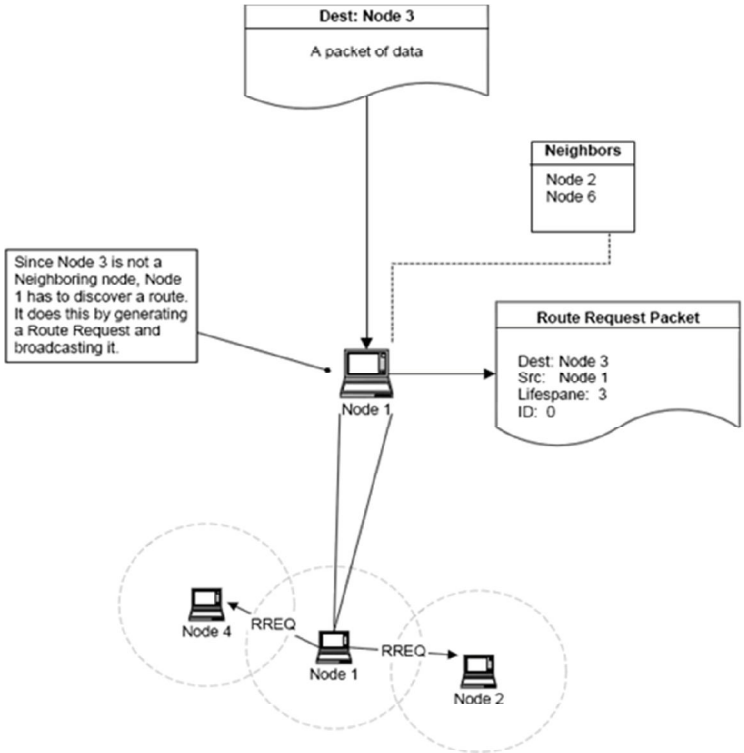

Figure 7. Nodes with Routing Table

In above fig.7 shown Node 1 wishes to send a message to Node 3. Node 1's Neighbours are Nodes 2 + 4. Since Node 1 cannot directly communicate with Node 3, Node 1 sends out a RREQ. The RREQ is heard by Node 4 and Node 2. But node 2 and node 4 send RREQ to its neighbours, if it found then sends RREP to source.

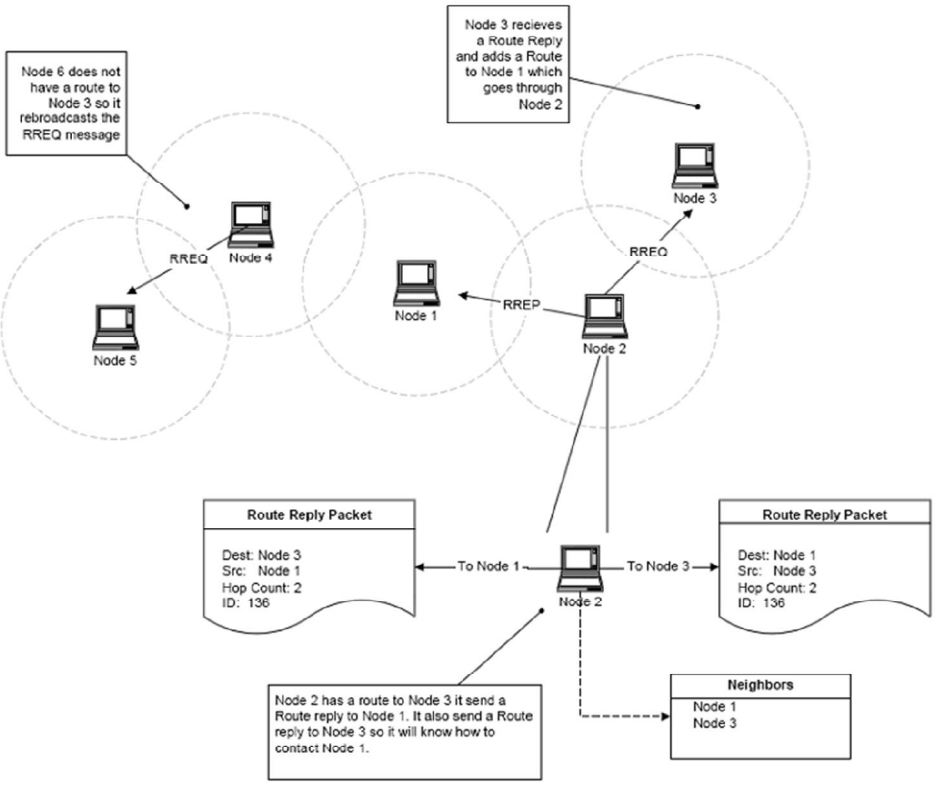

Figure 8. Rout Request

As above shown in Fig. 8 Node 2 has a route to Node 3 and replies to the RREQ by sending out a RREP. Node 4 on the other hand does not have a route to Node 3 so it rebroadcasts the RREQ. Node4 having the node 5 neighbour in which it is also not destination.

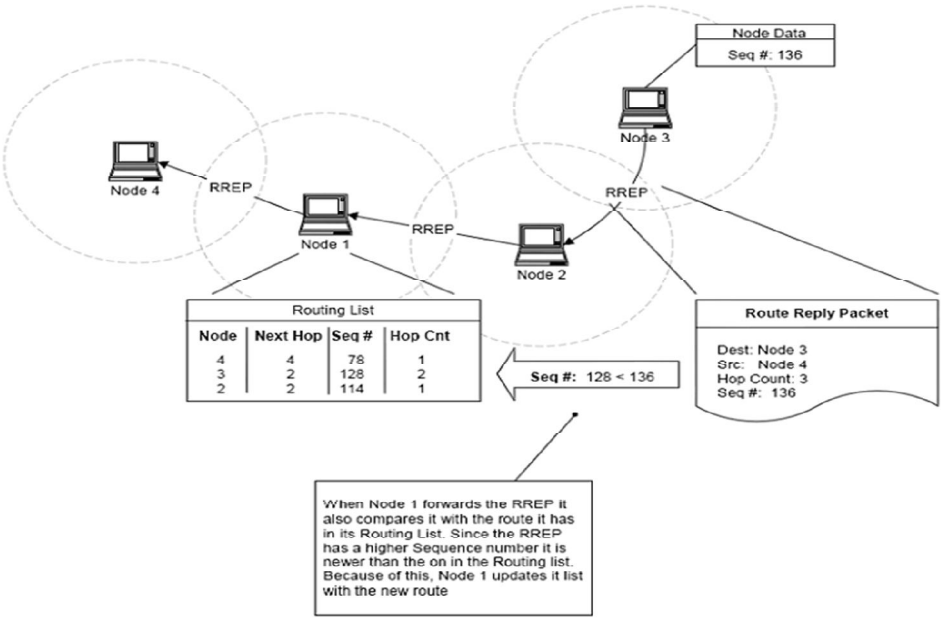

Figure 9. Route Reply

In the above Fig. 9, Node 1 is forwarding a RREP to Node 4. It notices that the route in the RREP has a better Sequence number than the route in its Routing List. Node 1 then replaces the route it currently has with the route in the Route Reply.

IV. SIMULATIONS

Simulation Environment
As given below in table 1, describes the simulation environment and the set for network scenario for our project.

TABLE I: SIMULATION ENVIRONMENT

Simulator	NS-2.26
Routing Protocols	AODV,SMT
Traffic Type	CBR(Constant Bit Rate)
Simulation Time	50 seconds
Number of Nodes	50
Maximum Connections	10, 20, 30, 40, 50
Rate	2.0ms
Area of Network	1000 X 1000
Radio Propagation Model	Two WayGround
Antenna Model	OmniAntenna
Attack Type	Ret, selfish

A. Performance Metrics

Delivery ratio: The ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination.

$$\text{Packet delivery ratio} = \frac{\text{Number of packet received}}{\text{Number of packet send}}$$

The greater value of packet delivery ratio means the better performance of the protocol.
Overhead: Refers to the time it takes to transmit data of packets in network. Each packet requires extra bytes of format information that is stored in the packet header, which, combined with the assembly and disassembly of packets, reduces the overall transmission speed of the raw data.

$$\text{Overhead} = \frac{\text{Time at packet receive}}{\text{Time at packet sent}}$$

Total Overhead: Refers to the total time it takes to transmit data of packets in network. It includes transmission overhead, network overhead, packet overhead, delay overhead etc. These factors make effects to decrease the performance of network while transmitting packets.

$$\text{Total Overhead} = \frac{\text{Total time taken to receive packet}}{\text{Time taken to send packet}}$$

B. Simulation Results of MAODV with No Attack

As shown in table 2, results are taken with respective without any Attack of malicious behaviour with varying number of connections (10,20,30,40,50). The fig.10 shows the network scenario for number of nodes

TABLE II : PERFORMANCE METRICS WITH NO ATTACK

Protocol Type – MAODV with No Attack			
Connections	Delivery- Ratio	OverHead	Total Over Head
10	0.969423	2878	1.031541
20	0.980518	7464	1.019869
30	0.974711	7236	1.025945
40	0.961465	6206	1.040079
50	0.997045	6051	1.002964

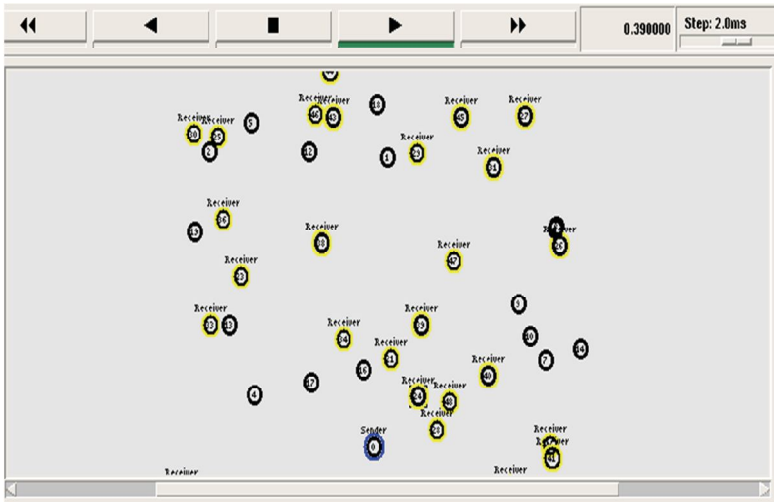

Figure 10. Initial network scenario with No Attack

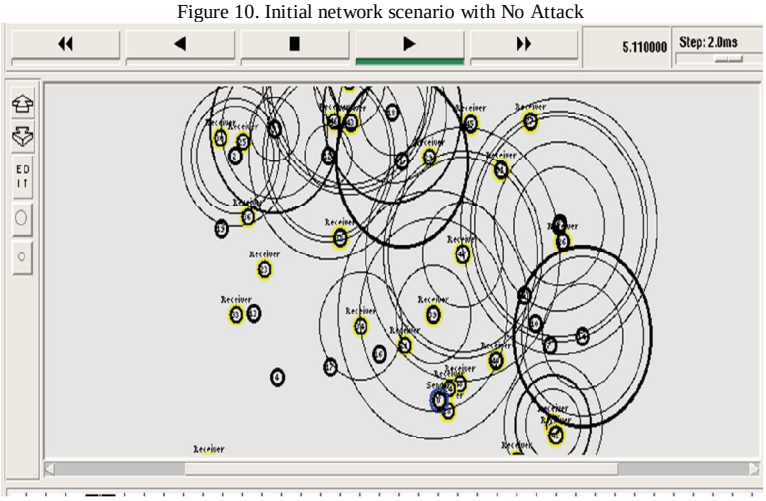

Figure 11. Simulation scenario

for varying number of connections in Network Simulator, in which the nodes with yellow colour acts as receivers and fig.11 shows how network is established between nodes in its communication range when simulation is started in NS2.Results outcome with performance of MAODV with respect to the Delivery Ratio, Overhead and Total overhead. In which above graph is plotted with Delivery ratio performance metric. In above Fig.12 which shows the graph, plotted with Receiver vs Delivery Ratio of No Attack, Attack and Detect. In which delivery ratio of No Attack and Detect gives near same view. In detect it gradually increase because it take time initially to detect unbehavior, node. But in Attack status between 10 and 20 node mobility is very low due to the dropping of packets. So after 20th node delivery ratio again improved.

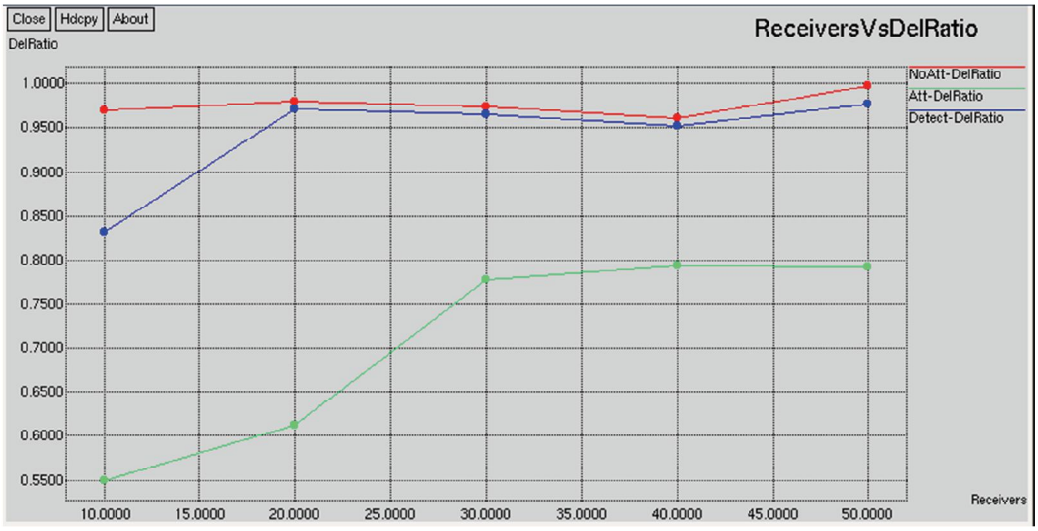

Figure 12: Average Delivery vs Receivers of MAODV and SMT

C. Simulation Results of MAODV with Attack

TABLE III: PERFORMANCE METRICS WITH ATTACK

Protocol Type – MAODV with Attack			
Connections	Delivery- Ratio	Over Head	Total Over Head
10	0.549837	18982	1.818722
20	0.612173	9365	1.633525
30	0.777940	8912	1.285446
40	0.794018	8559	1.259417
50	0.792919	7683	1.261162

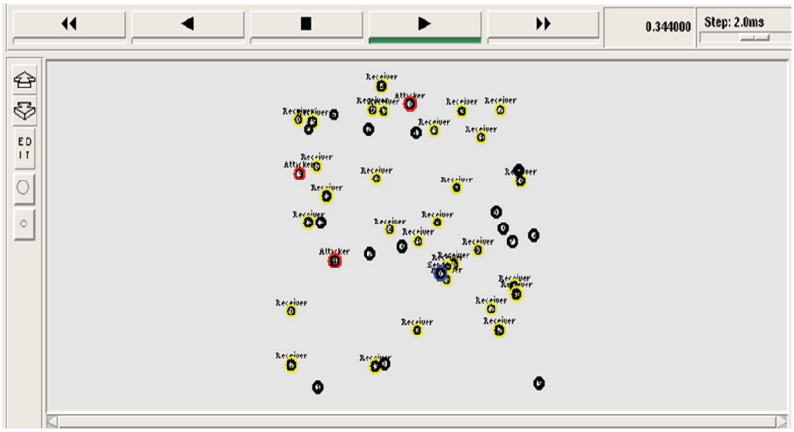

Figure 13. Initial scenario with attackers

As shown in above table 3, results are taken with respective with Attack of malicious behaviour with varying number of connections (10, 20, 30, 40, 50). The above Fig.13 shows the network scenario for number of nodes for varying number of connections in Network Simulator window before simulation and Fig.14 shows how network is established between nodes in its communication range when simulation is started in NS2 we can observe packet drop in this figure. Results outcome with performance of normal AODV with respect to the Delivery ratio, Overhead and Total overhead. In above Fig.15 which shows the graph plotted with Overhead performance metric. According to above results graph is plotted with Receiver vs Delivery Ratio of No Attack, Attack and Detect. In which over congestion of packets Overhead is high with Attack.

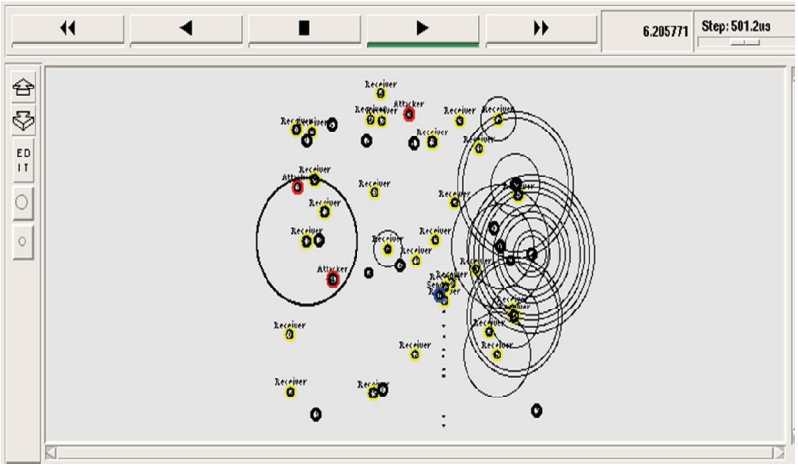

Figure 14. Simulation scenario with dropping of packet

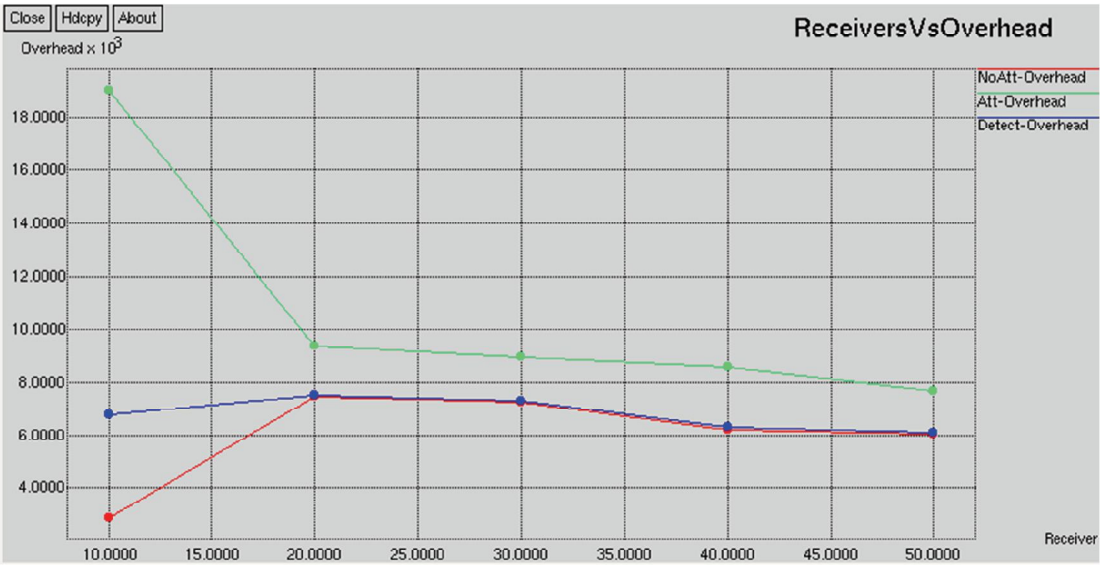

Figure 15. Average Overhead vs Receivers of MAODV and SMT

D. Simulation Results for MAODV with SMT Detect

TABLE IV: PERFORMANCE METRICS WITH DETECT

Protocol Type –SMT with Detect			
Connections	Delivery- Ratio	Over Head	Total OverHead
10	0.831912	6776	1.183830
20	0.970518	7494	1.029869
30	0.964711	7276	1.032594
40	0.951465	6306	1.050079
50	0.977045	6091	1.012964

As shown in above table 4, results are taken with respective with Detection of malicious behaviour with varying number of connections (10, 20, 30, 40, 50). The above Fig.16 shows the network scenario for number of nodes for varying number of connections in Network Simulator and shows how network is established between nodes in its communication range when simulation is started in NS2.Results outcome with performance of SMT with respective to the Delivery Ratio, Overhead, and Total overhead. In which above Fig.17 shows the graph which is plotted with respective Total overhead performance metric.

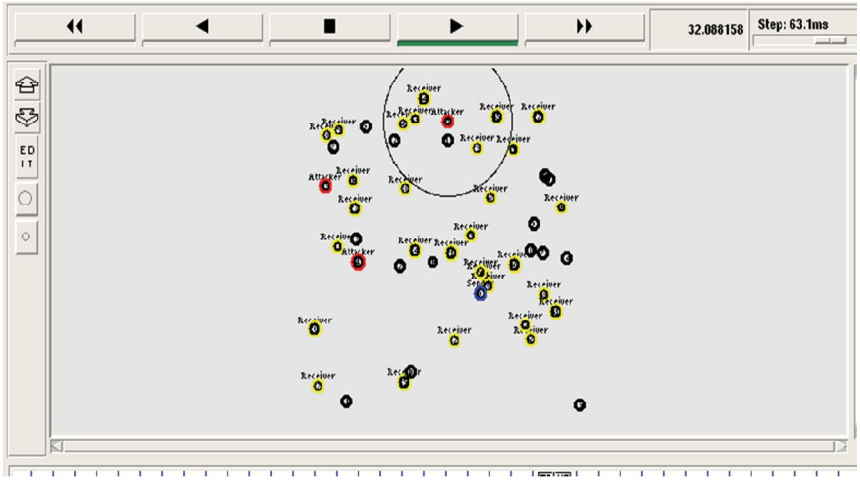

Figure 16. Simulation with detect

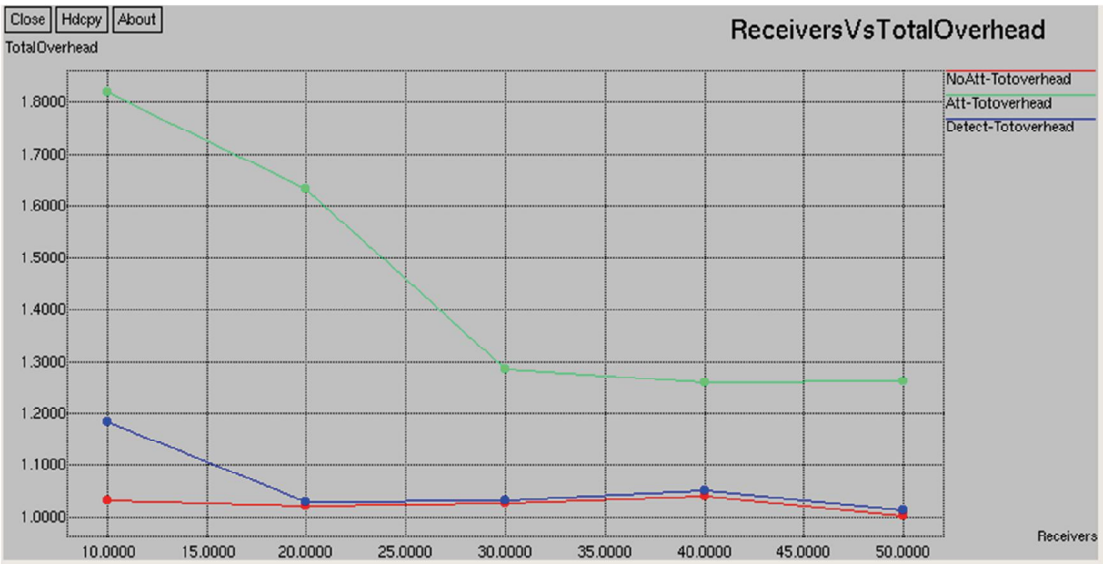

Figure 17: Average Total overhead vs Receivers of MAODV and SMT

According to above results graph is plotted with Receiver vs Total overhead of No Attack, Attack and Detect. In which over congestion of packets Total overhead is after detection of malicious nodes with Attack. But as compare to MAODV, the SMT after detection of attacks is same. Because initially nodes to be detected due to this some congestion initial it will take time with low total overhead.

V. Conclusion And Future Work

In this work we have made normal Unicast AODV to Multicast AODV operation in which SMT Agent is implemented to detect attacks and results can be extracted in terms of Delivery Ratio, Overhead and Total overhead. Simulation results are taken using Network Simulator 2.26 Under scenario varying number of connections. Due to presence of multicast and queues, MAODV show better performance over detecting attackers using SMT Agent. Since routing information is updated and multicast frequently, MAODV with attacks performance degrades as number of connections increases, compared to as that of MAODV without attacks and after detection using SMT Agent. MAODV performs better as high mobility scenarios, low overhead and total overhead from our simulation. So from all analysis we finally conclude that MAODV with SMT protocol implementation is the ideal choice for communication.

The work that has been accomplished in this project is quite flexible, as multiple nodes can be accessed data from tcl script and bringing the possibility to modify the existing protocols to adapt to multicast support mobile node architecture. One additional aspect would be the extension of whole model so as to really include multicast technologies, and not only multicast belonging to same technology. Another topic would be to address is in our project results are carried out varying only number of connections with random connection, in future we can consider results by varying speed with fixed position so that performance may vary this could also benefit for the new feature. Also multicast operation can be extended for other routing protocol like DSDV, TORA etc.

REFERENCES

[1] Todd R Andel "Surveying security analysis techniques in MANET" IEEE Communication surveys, The Electronic Magazine of Original Peer-Reviewed Survey Articles, vol 9, No4, 2007.

[2] Christopher N. Ververidis and George C. Polyzos, "Service Discovery for Mobile AdHoc Networks", IEEE Communications Surveys & Tutorials, vol 10, No 3, 2008.

[3] Loay Abusalah, Ashfaq Khokhar and Mohsen Guizani "A Survey of Secure Mobile AdHoc Routing Protocols", IEEE Communications Surveys & Tutorials, vol 10, No 4, 2008.

[4] Yu wang, xiang-yang Li, wen-zhan, "Energy Efficient Localized Routing in Random Multihop Wireless Network", IEEE Transactions on Parallel and Distributed Systems, vol 22, No 8, 2011.

[5] Karim ElDefrawy, Gene Tsudik "Privacy- preserving Location based on demand routing in MANETs", IEEE Journal on selected area in communications, vol 29, No 10, Dec 2011.

[6] Wei wang, Boon-Hee Soong, "Collision-free and Low latency scheduling algorithm for Broadcast operation in wireless AdHoc networks", IEEE Communication Letters, vol 11, No 10, Oct 2007.

[7] Suhua Tang and Bing Zhang, "A Robust AODV protocol with local update", ATR Adaptive communications research lab, Japan.5th International Symposium on multi dimentional mobile communication Proceedings, vol 1,sept 2004

[8] Adel S El asheb, "Performance evaluation of AODV and DSDV routing protocol in wireless sensor network environment", International conference on Computer Networks and Communication Systems, vol 35, 2012.

[9] Humaira Nishat, Vamsi Krishna, "Performance evaluation of AODV and Modified AODV (R-AODV) in MANETs", International journal of Distributed and Parallel Systems, vol 2, No1, Jan 2011.

[10] M.Devi and Dr. V. Rhymend Uthariaraj, "Routing with AODV protocol for Mobile AdHoc network" International Journal of Technology And Engineering System, vol 2, No 1, March 2011.

[11] Mehul Revankar, "Attacks in Ad-Hoc Networks and Modeling in NS-2" ,ECE 746.